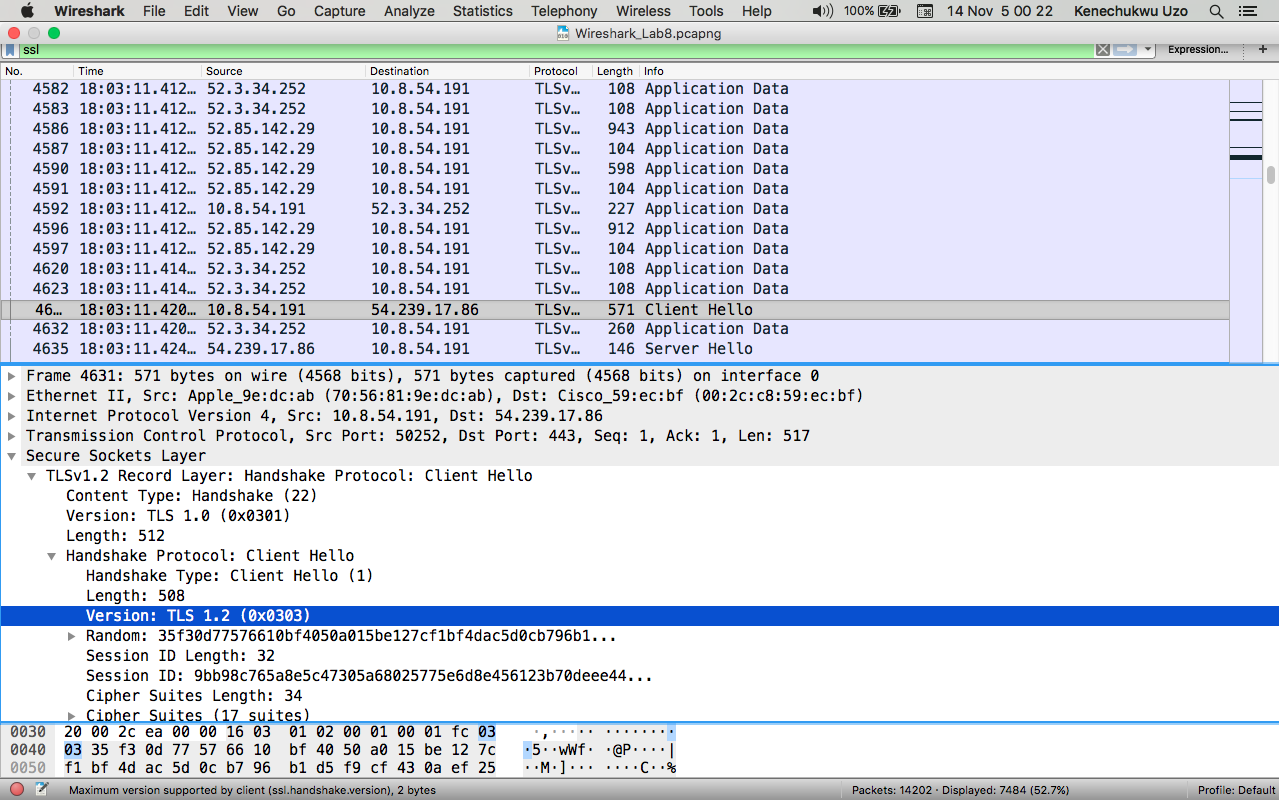
Lab 8 - SSL/TLS

Chibunze Uzo

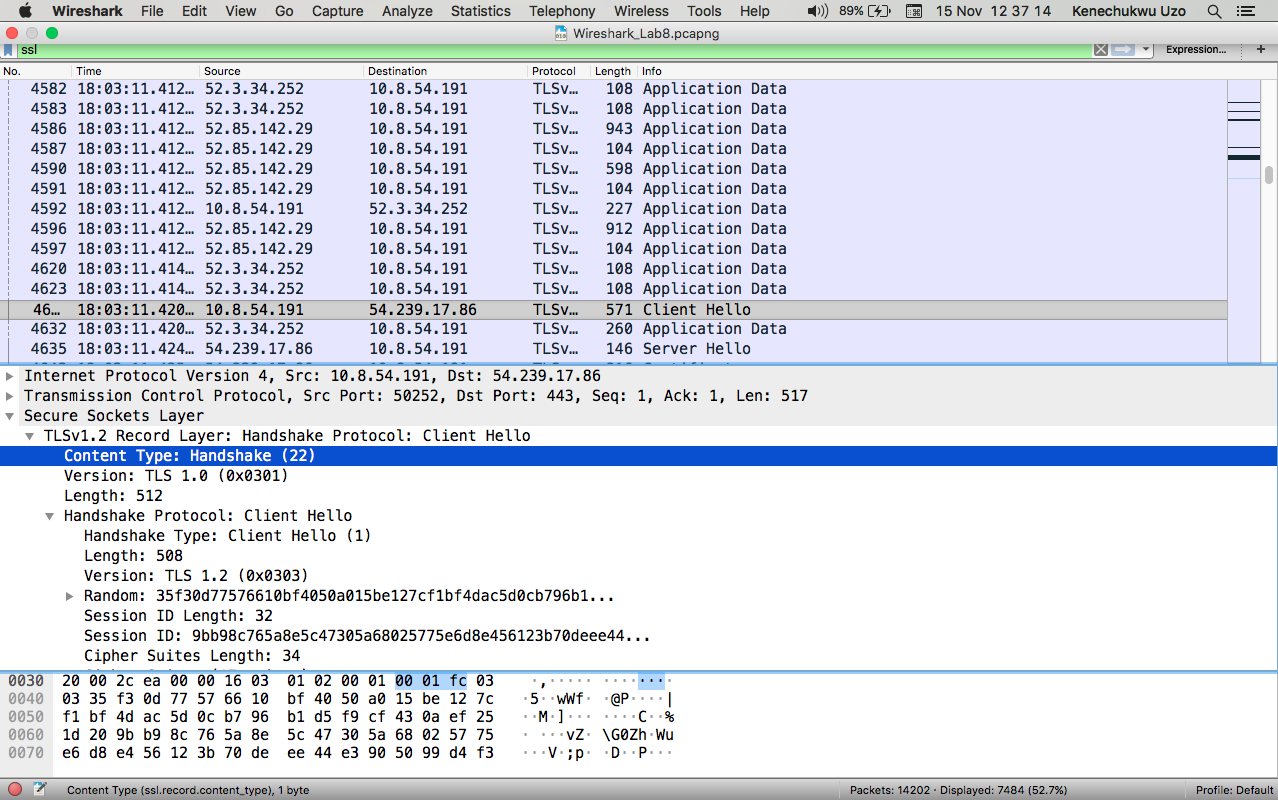


**Client Hello Record:**

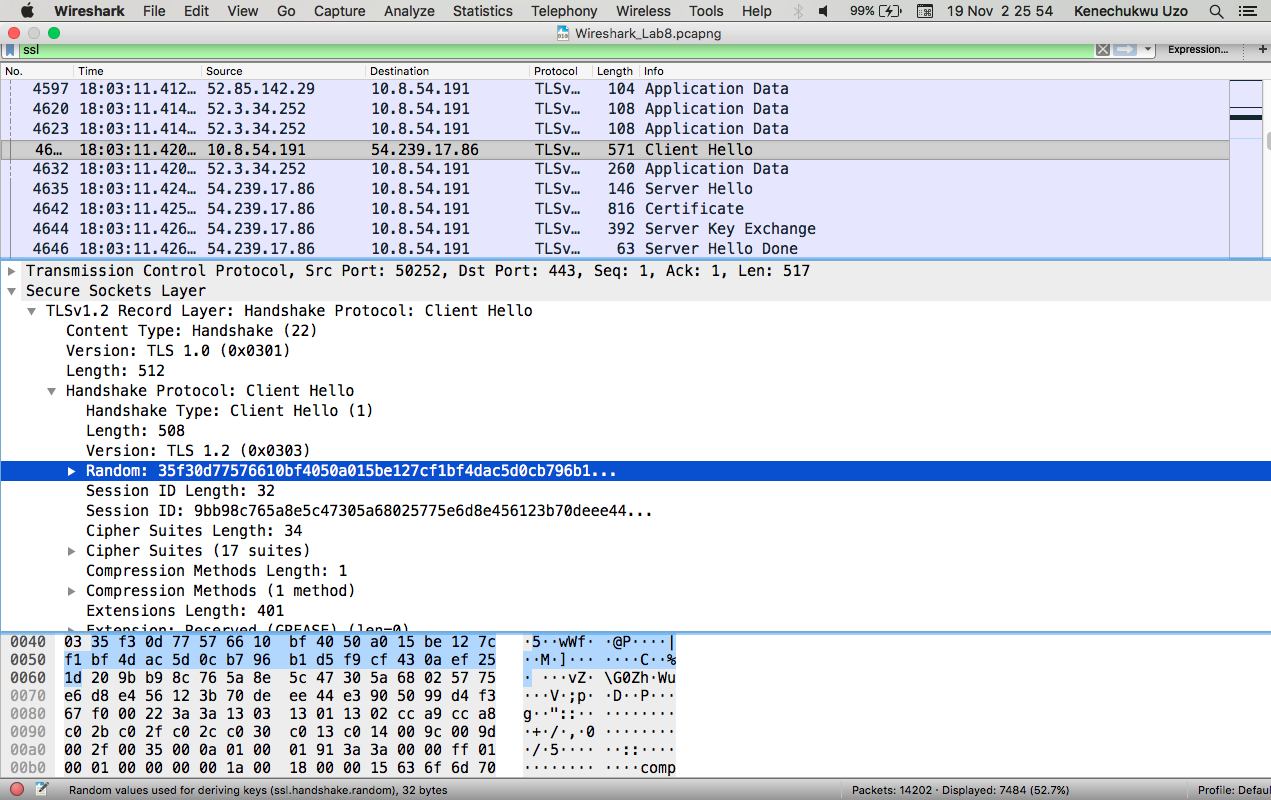
1. **The version is TLS 1.2**



2. The Content Type: **Handshake (22)**



3. **35:f3:0d:77:57:66:10:bf:40:50:a0:15:be:12:7c:f1:bf:4d:ac:5d:0c:b7:96:b1:d5:f9:cf:43:0a:ef:25:1d**

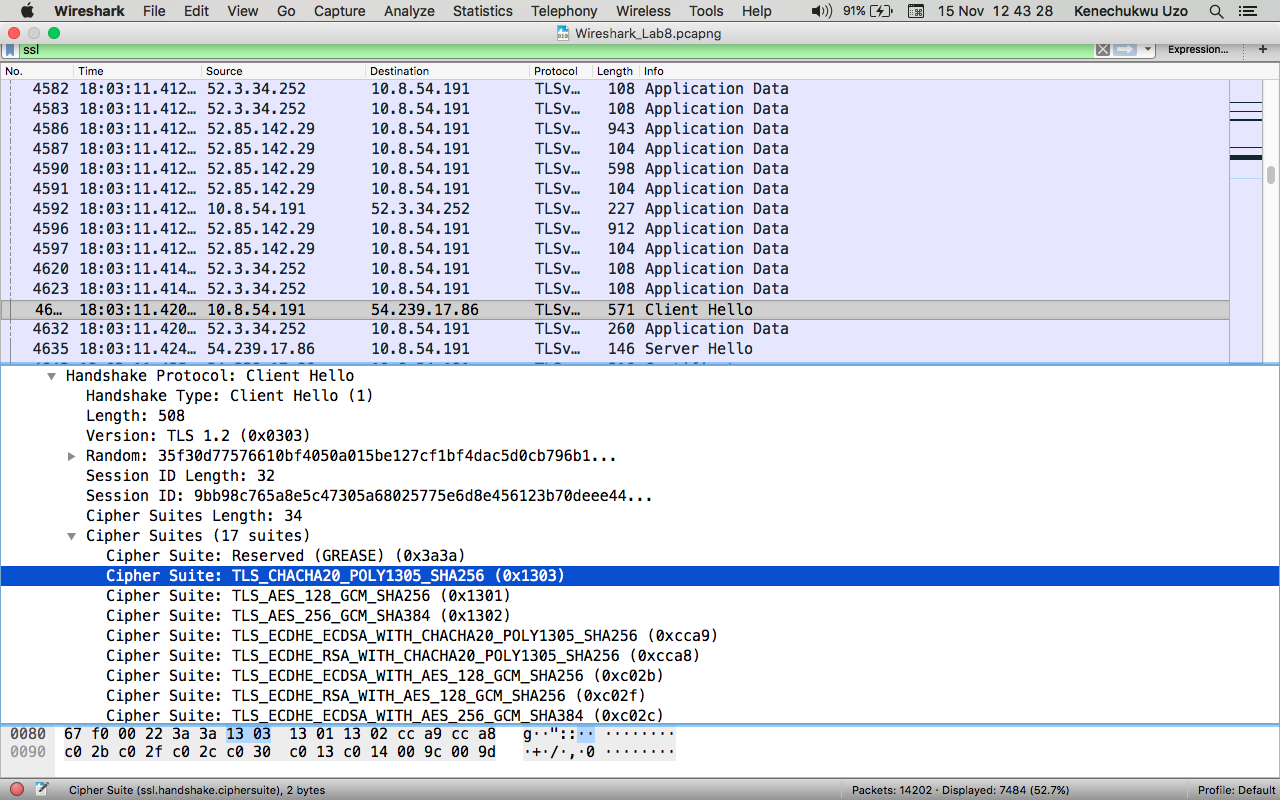


4. **Yes it does, Cipher Suite:**

**Public key algorithm : CHACHA20**

**Symmetric - key Algorithm : POLY1305**

**Hash algorithm : SHA256**



**Server Hello Record:**

1. **Yes it does, Cipher Suite:**

**TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0XC013)**

